International Journal of Advanced Research in

Computer Science Engineering and Information Technology

Volume: 1 Issue: 2 12-Sep-2013,ISSN_NO: 2321-3337

AN ENHANCED HIGH LEVEL USER AUTHENTICATION AND DATA SECURITY USING BIOMETRIC INPUT

P.Kannan* , Karthikeyan.P**
School of Information Technology and Engineering,
VITUniversity.Vellore
pkarthikeyan@vit.ac.in , ***sreekannan2011@gmail.com***

***Abstract**—The main impact of the project proposal is from the concept of "Getting Biometric input from the user without using any external devices for providing high level user authentication during login". The purpose of biometric recognition for secure access restricts is to avoid the un-trusted source of interaction.Most cases, object level changes happening in the IT environment is not monitored properly. Considering, a Database Administrator is trying to change an object. In that case, he will change without the knowledge of other DBA's. In case of accidental changes, or any changes in the system acceptance of the other administrator is important. The system may be prone to hacking vulnerabilities too. To overcome the above issues, we are proposing a standard technique to avoid hacking with the help of Biometric input. Once the user is trying to access the objects to do any changes in the databasethen biometric system will decide the authentication part.*

Keywords—Biometric input, Data Base Administrator (DBA), Private key, Public Key, Object Changes.

I. INTRODUCTION

In all organization they are maintaining separate server to maintain database, related to the company in huge manner. For that based on the organization standards administrator having responsibilities to maintain the data in database. Admin having the full rights to access the database and they can even do the changes in the system but the main thing if there is more than one admin for that system each one need to approve the changes then only that changes will be reflected successfully in that system that is mentioned here as object level changes. Admin is usually have the sign in facility to access the database that were giving username and password in now a days it is not enough to get pass only in one checkpoint like password because it high risk that hackers have chances to get the password in any manner even though they were encrypted so while sign in checkpoints for the admin approval is need to be increased. For that in this proposal of the project is to make high level authentication and secure the data efficiently.

Authentication takes place in three different levels

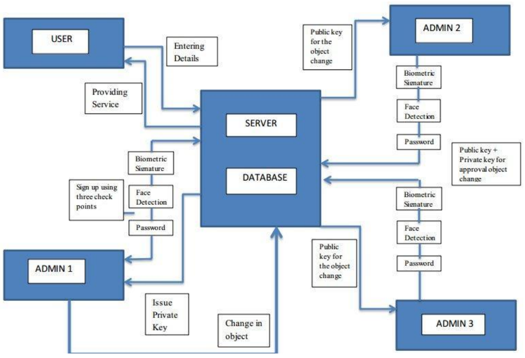
First level: Here admin need to give the username and password to know about the specific admin is logging in this level ensures correctly. Then password is encrypted and stored in database. Here two main algorithm are used for encryption is RC2 algorithm and Triple DES algorithm. In RC2algorithm they are some mandatory fields needed before encryption it needs private key that key is generated by using Triple DES algorithm this makes high efficiency encryption in saving password in database while decryption same private key needed to be used no hackers can figure out the password in this manner.

Second Level: Admin face is detected using the webcam for that during sign up itself admin needed to provide all the necessary details and face of admin will be detected and stored in future authentication the face recognition will be processed if it matches then only admin can move on to next level.

Third Level: This level mainly based on the new concept of using biometric input but without any external devices they needed to be done for that only way toget input from the admin itself they can manually draw the digital signature for that lines and circles are there to use and even colour pallets is provided to choose the admin favourite colour for the digital signature here admin need to be more precautious while drawing for future sign in and al admin needed to use the same signature for authentication. If admin is not sure in biometric signature during sign up, forgot signature facility is also added here private key that were already mail to admin that key need to placed here after that new biometric signature will be obtained again from admin later they can use this new signature for the authentication.

II. DESIGN METHODOLOGY

This system is designed with .Net as framework using sample application that is developed it might be used for all purposes where many administrators can access the application but they should be authenticated and clear the all the three checkpoints then only administrator can enter into the application and change the object in the system. Here application is simulated and object changes in the system are checked and changes are reflected successfully in the database.



A. *System Architecture*

III. PROPOSED NEW IDEA

All the information regarding user and details about the organization are maintained in the database and to access the database admin will have full rights to maintain and they have permission to change in the tables if hacker break the password of the admin and enters in the system as the admin then all the data can be get hacked. To secure from that here we provide the high level authentication each admin should cross the three check points that were efficiently designed and that can't be predicted by the hacker. Then object level changes that occur in the system must be so secured and before the changes applied in the system it should be approved by all admin here we provide new technique using public key other admin are notified about the change and they asked to approved if the changes are need in the system.

IV. FUNCTIONALITY EXPLANATION

A. Authentication process

In this module while configuring new system in the organization all the admin need to enter the details while sign up and that mean time after creating the new credentials private key that were generated will be send to admin mail id that will be used if admin forgot password or forgot signature and in future use if object changes had occurred admin can make use of that private key. That private key is generated using the triple DES algorithm. While sign in admin need to give username and password for providing first level of security here encryption and decryption technique is done by using RC2 algorithm for this algorithm private key is essential before encryption for that private key is different for each admin by using that encryption is taken place so that no hacker can break the security and guess the password for the admin this provides strong security authentication for the administrator.*B. Face Detection And Recognition*

This is the second level of authentication by using this face detection and recognition concept it might be useful to check whether the certain user is login or not in the system. After the admin registering details for the authentication then admin face will be detected and stored by using web camera. Then during sign in only that admin can enter easily then move on to the next level in authentication. By using these standard methods only high level authenticated is getting strong.

C. Biometric Key Generation

We are proposing an innovative approach in defining the Biometric keys with the help of geometric designing of signing the key for a specific user. To overcome expensive hardware, we've come up with an innovative approach of creating this kind of signatures and it will be validated on each steps of the signature.Administrator itself needed to design the signature for the third level of authentication. If the users have forgotten the signature, he is able to re-generate the key at requests. This digital signature concept make sure that only the same person can put the same signature again and again this ensure the admin authentication level in high standards. In addition while signing admin given choice to choose to colours from colour palette. Only lines and circles are given by using that only admin can design the digital signature.

D. Administrator Functionalities

In this admin module new features are added like checking the mail Inbox for the private key credentials that provided while sign up. Then for object changes they will provide the public key that can also check here in mail with other official mail are also there in mail. The registered user and there details are listed here for admin checking if needed they can be rejected. Acceptance of the user will be provided with username and password that also mailed to the user.

E. Object Change

Based on the access provided, the administrator is allowed to change the objects.The main changes is anyway going to happen in the tables so based on the user decision table that is dependent in the system will be easily modified. That will be done by using the DML statements to make changes like insert, delete, drop, add and rename tables in the database is done by the admin. After immediately change public key is auto generated send mail to other admin.The main thing in organization is not only having the single admin to accept the changes immediately it depends on each one admin decision. So for that changes done by the admin should be notify to other admin and they must also accept the changes and modification in the table then only changes will be reflected successfully.

F. Public Key Access

Once the administrators have done some object change an automatic 16 bit length of public key is created using Triple DES algorithm that relevant to the object change is done in system.An automatic emailwill be generated and it's sent to the other administrator with the public key. In addition, the administrator will be validated with the Biometric checks for the authentication.That key is so confidential and that must be keep secured because after inserting the correct key only other admin can see the changes otherwise they can't see accept the changes.

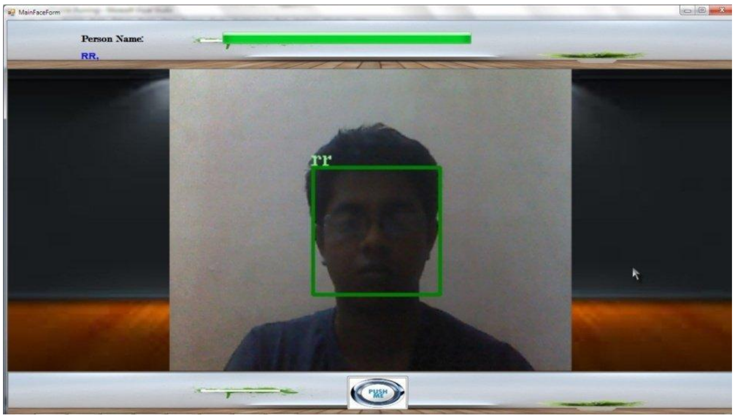
G. Object Change Confirmation

Once the key is generated and administrator authentication process with the biometric checks, the administrator is requested to apply the key in the Key apply module. The public key should be applied in the exact format even there are small changes it will not accept the key. Not only the public key then also private key for the separate user also given in the required field these fields are mandatory and checked for the assurance about the admin. Once if all the administrators approve through their public and private keys, the changes will be reflected in the system.

H. Results and Discussion

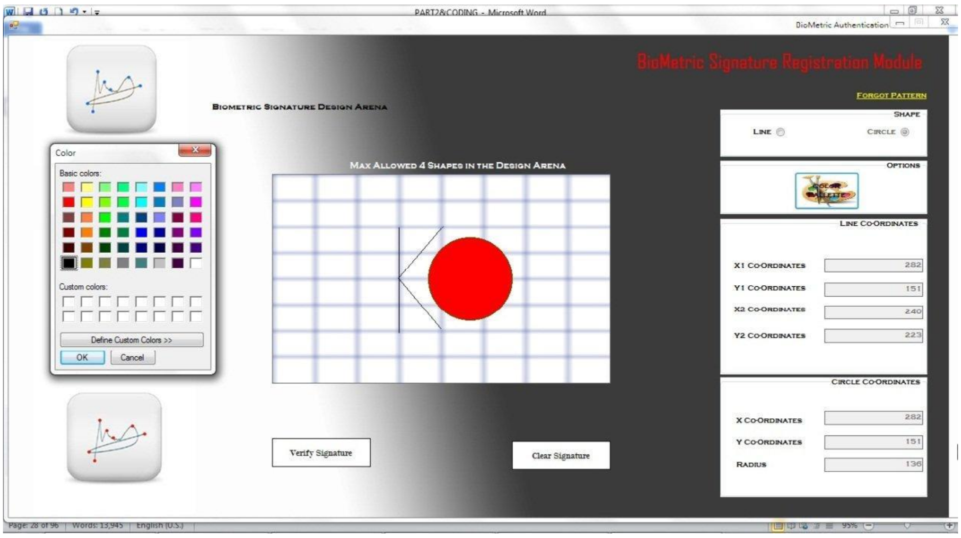
Providing high level security to secure large data in the organization is the main part in this paper. For that three level for the authentication is provided and monitoring data changes in the system for that each provided with different cases to consider before the changes made by the admin. They are having full responsibilities to maintain the database in efficient manner. In that authentication levels makes strong in the system only the certain admin can login if any other used to login might lead to restriction in face recognition. Others cannot access the application and change the object in this application all the authentication level are highly secured and protected.

V. SNAPSHOTS



Person Name:
RR.

Fig. 1 Face Recognition


PART2&CODING - Microsoft Word
DioMetric Authentication
BioMetric Signature Registration Module
Biometric Signature Design Arena
Color
Basic colors:
Custom colors:
Define Custom Colors >>
OK
Cancel
Max Allowed 4 Shapes in the Design Arena
Verify Signature
Clear Signature
Forgot Pattern
Options
Color Pallette
Page: 28 of 96 | Words: 13,945 | English (U.S.)
95%

Shape
Line ○ Circle ●

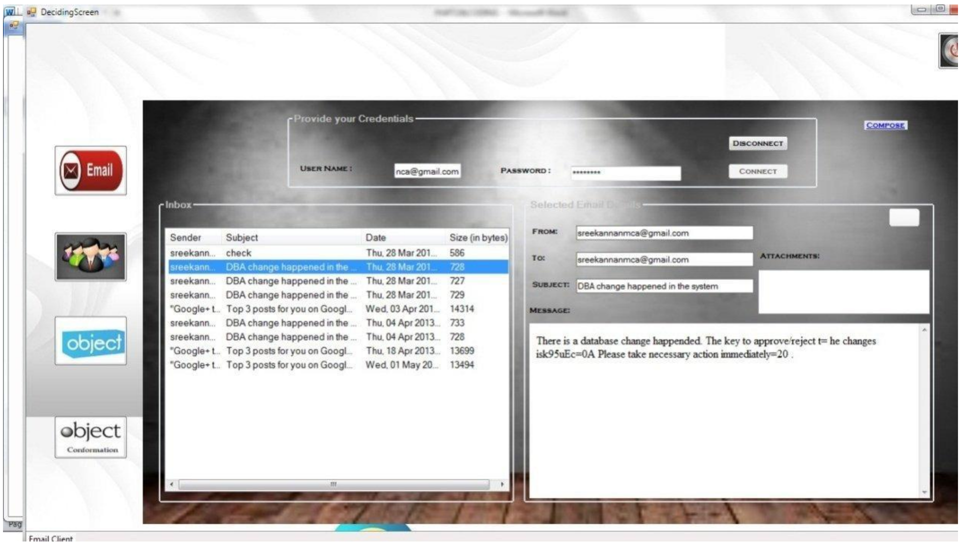
Line Co-Ordinates

X1 Co-Ordinates 282
Y1 Co-Ordinates 151
X2 Co-Ordinates 240
Y2 Co-Ordinates 223

Circle Co-Ordinates

X Co-Ordinates 282
Y Co-Ordinates 151
Radius 136

Fig. 2 Biometric Input



USER NAME : nca@gmail.com

PASSWORD : ********

Sender	Subject	Date	Size (in bytes)
sreekann...	check	Thu, 28 Mar 201...	586
sreekann...	DBA change happened in the ...	Thu, 28 Mar 201...	728
sreekann...	DBA change happened in the ...	Thu, 28 Mar 201...	727
sreekann...	DBA change happened in the ...	Thu, 28 Mar 201...	729
"Google+ t...	Top 3 posts for you on Googl...	Wed, 03 Apr 201...	14314
sreekann...	DBA change happened in the ...	Thu, 04 Apr 2013...	733
sreekann...	DBA change happened in the ...	Thu, 04 Apr 2013...	728
"Google+ t...	Top 3 posts for you on Googl...	Thu, 18 Apr 2013...	13699
"Google+ t...	Top 3 posts for you on Googl...	Wed, 01 May 20...	13494

FROM: sreekannanmca@gmail.com

TO: sreekannanmca@gmail.com

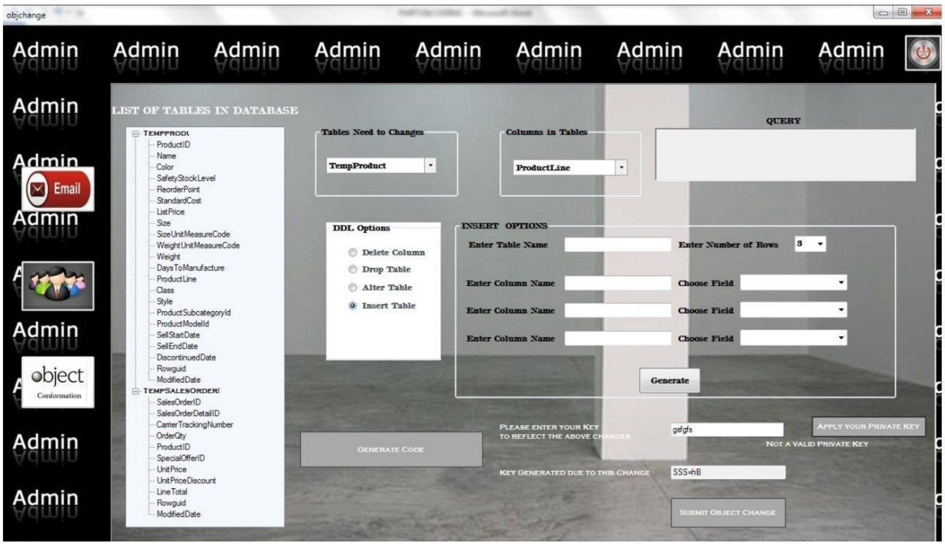
SUBJECT: DBA change happened in the system

ATTACHMENTS:

MESSAGE:

There is a database change happended. The key to approve/reject t= he changes isk95uEc=0A Please take necessary action immediately=20 .

Fig. 3 Administrator Checking E-Mail



- TEMPPRODI
  - ProductID
  - Name
  - Color
  - SafetyStockLevel
  - ReorderPoint
  - StandardCost
  - ListPrice
  - Size
  - SizeUnitMeasureCode
  - WeightUnitMeasureCode
  - Weight
  - DaysToManufacture
  - ProductLine
  - Class
  - Style
  - ProductSubcategoryId
  - ProductModelId
  - SellStartDate
  - SellEndDate
  - DiscontinuedDate
  - Rowguid
  - ModifiedDate
- TEMPSALESORDERI
  - SalesOrderID
  - SalesOrderDetailID
  - CarrierTrackingNumber
  - OrderQty
  - ProductID
  - SpecialOfferID
  - UnitPrice
  - UnitPriceDiscount
  - LineTotal
  - Rowguid
  - ModifiedDate

Tables Need to Changes: TempProduct

Columns in Tables: ProductLine

DDL Options

○ Delete Column
○ Drop Table
○ Alter Table
● Insert Table

INSERT OPTIONS

Enter Table Name:
Enter Number of Rows: 3
Enter Column Name: Choose Field:
Enter Column Name: Choose Field:
Enter Column Name: Choose Field:

PLEASE ENTER YOUR KEY TO REFLECT THE ABOVE CHANGES: gsfgfs

NOT A VALID PRIVATE KEY

KEY GENERATED DUE TO THIS CHANGE: SSS=hB

Fig. 4 Object Changes

VI. CONCLUSIONS

This work tackles the high level user authentication and monitoring object changes in the system to maintain these above operations this project is developed and one of the advanced and new level biometric authentication process is done but without using any biometric devices, getting input from the user in a digital signature format makes strong on the high level user authentication. It is mainly used as the future concept that can be used in any application but here admin side this biometric input is used because of admin having more responsibilities to remember the input that is given while registration. Other important concept is object level changes in the application by admin should get permission and acceptance of all other admin that are involved in the organization to avoiding conflict in the organization regarding the object changes are not valid like that after approval of all admin only object changes reflected successfully in the system. But still studies in the biometric using external are facing open problem but this integrated biometric concept may overcome that problem.

REFERENCES

[1] Carlos Vivaracho-Pascual and Juan Pascual-Gaspar, *On the Use of Mobile Phones and Biometrics for Accessing Restricted Web Services,*ieee transactions on systems, man, and cybernetics—part c: applications and reviews, vol. 42, no. 2, march 2012.

[2] .Q. Tao and R. N. J. Veldhuis, *Biometric authentication for a mobile personal device*, in *Proc.* 3rd Annu. Int. Conf. Mobile Ubiquitous Syst.Netw. *Serv.*, Jul. 2006.

[3] SidaLin ,QiXie, *A secure and efficient mutual authentication protocol using hash function***,** 2009 International Conference on Communications and Mobile Computing.

[4] Andreas Holzinger, Regina Geierhofer, Gig Searle, *Biometrical Signatures in Practice: A challenge for improving Human- Computer Interaction in ClinicalWorkflows*, Mensch & Computer 2006.

[5] F. Alonso-Fernandez, J. Fierrez-Aguilar, J. Ortega-Garcia, and J. Gonzalez-Rodriguez, *Secure access system using signature verification over tablet PC*, IEEE Aerosp. Electron. Syst. Mag., Apr. 2007.

[6] J. M. Pascual-Gaspar, V. Carde˜nosoPayo, and C. E. Vivaracho- Pascual, *Practical on-line signature verification*" in Proc. 3rd Int. Conf.Adv. Biometr. Berlin, Heidelberg, Germany: Springer-Verlag, 2009.

[7] N. L. Clarke and S. M. Furnell, *Advanced user authentication for mobile devices*, Comput. Secur., vol. 26, no. 2, pp. 109–119, 2007.

[8] *Enhancing security for the mobile workforce*, Biometric Technol. Today,vol. 16, no. 1, pp. 8–8, 2008.

[9] Sarker, M.Z.H, Parvez, M.S, *A Cost effective symmetric key cryptographic algorithm for small amount of data*, 9th International Multitopic Conference, IEEE INMIC 2005.

[10] Sharafat, A.R, ;Dept of Electr. &Comput. Eng., Waterloo Univ., Tahvildari, L., *A Probabilistic approach to predict changes in object-oriented software systems*. Software maintainance and Reengineering, 2007. CSMR '07. 11th European Conference.